**TENABLE.AD**

UPDATE PROCEDURE – TLS

---

### a. Document contributors:

<table>
<thead>
<tr>
<th>Author</th>
<th>Qualification</th>
<th>Contact address</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENABLE</td>
<td>DevOps team</td>
<td><a href="https://community.tenable.com/s/">https://community.tenable.com/s/</a></td>
</tr>
</tbody>
</table>

### b. Document history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date (dd/mm/yyyy)</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.0</td>
<td>12/07/2019</td>
<td>ALSID</td>
<td>Initial document</td>
</tr>
<tr>
<td>2.5.0</td>
<td>23/10/2019</td>
<td>ALSID</td>
<td>Update for 2.5.0</td>
</tr>
<tr>
<td>2.6.0</td>
<td>19/02/2020</td>
<td>ALSID</td>
<td>Update for 2.6.0</td>
</tr>
<tr>
<td>2.6.1</td>
<td>05/03/2020</td>
<td>ALSID</td>
<td>Update for 2.6.1</td>
</tr>
<tr>
<td>2.6.3</td>
<td>04/04/2020</td>
<td>ALSID</td>
<td>Update for 2.6.3</td>
</tr>
<tr>
<td>2.7.0</td>
<td>06/06/2020</td>
<td>ALSID</td>
<td>Update for 2.7.0</td>
</tr>
<tr>
<td>3.0.0</td>
<td>01/12/2020</td>
<td>TENABLE</td>
<td>Update for 3.0.0</td>
</tr>
<tr>
<td>3.1.0</td>
<td>02/08/2021</td>
<td>TENABLE</td>
<td>Update for 3.1.0</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

Introduction 3
   Document objectives 3
   Abbreviations 3
   Infrastructure presentation 3
      Network Overview 3
   Prerequisites 6
      Minimal configuration 6
      Additional support information 6
      Installation programs 7
         Deployment on Windows Server (Full-Desktop Experience) 7
         Deployment on Windows Server Core 7
Update PROCEDURE 7
   Backup your system 8
   Update Directory Listener 8
   Start Directory Listeners services 9
Active Directory configuration 9
   General considerations 10
   Access to specific Active Directory objects or containers 11
   Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack 11
      Tenable’s deployment script 11
         Synthesis of the technical changes made by Tenable’s deployment script 12
      Microsoft Sysmon 13
         Manual deployment of Microsoft Sysmon on the domain controllers (optional) 14
      Problem with Advanced Audit Policy Configuration GPO precedence 15
      Update the Tenable module on the Domain Controllers 16
Annexes 17
   Optional Sysmon configuration file 17
1. **INTRODUCTION**

1. Document objectives

This document helps you perform a clean installation of Tenable’s on-premises solution in TLS Mode. The required component is the Directory Listener to target the audited domains.

Note: For many examples, the "E" partition letter will be used by default for data partition.

2. Abbreviations

The following table lists the abbreviations used in this documentation:

<table>
<thead>
<tr>
<th>Abbr.</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL / DLxx</td>
<td>Directory Listener</td>
</tr>
<tr>
<td>SEN / SENxx</td>
<td>Security Engine Node</td>
</tr>
<tr>
<td>DB / DBxx</td>
<td>Storage Manager</td>
</tr>
<tr>
<td>WI / WIxx</td>
<td>Web Interface, or any application offering a website</td>
</tr>
<tr>
<td>PC / PCxx</td>
<td>Personal Computer, or devices used as a computer</td>
</tr>
<tr>
<td>IoE / IoExx</td>
<td>Indicator of Exposure</td>
</tr>
<tr>
<td>DC / DCxx</td>
<td>Domain Controller</td>
</tr>
</tbody>
</table>

3. Infrastructure presentation

The following information is provided as a referral for this document. The infrastructure presented must be considered as a supported architecture.

3.1. Network Overview

The network is spliced across three areas. The following schema shows an overview of the network communication:
To go further, see the following schema and its associated network matrix. They describe each required protocol and port used by the Tenable platform:
The following network matrix describes each required protocol and port used by the Tenable platform.

<table>
<thead>
<tr>
<th>Network flows (From -&gt; To)</th>
<th>Tenable’s usage</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
</tr>
<tr>
<td></td>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
<td>UDP/53 and TCP/53</td>
</tr>
<tr>
<td></td>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS</td>
<td>TCP Dynamic (&gt; 1024)</td>
</tr>
<tr>
<td></td>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>Global Catalog</td>
<td>TCP/3268 and TCP/3269</td>
</tr>
<tr>
<td></td>
<td>Replication</td>
<td>RPC Endpoint Mapper</td>
<td>TCP/135</td>
</tr>
<tr>
<td>Tenable Security probe -&gt; Tenable for AD SaaS platform</td>
<td>Tenable security probe TLS Tunnel</td>
<td>Advanced Message Queuing Protocol encrypted in TLS</td>
<td>TCP/5671</td>
</tr>
<tr>
<td>End-users -&gt; Tenable for AD SaaS platform</td>
<td>Tenable end-user services (Web portal, REST API, etc.)</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
</tbody>
</table>
In addition to the Active Directory protocols, some additional flows may be required depending on Tenable’s platform configuration. These protocols and ports must be open between Tenable’s platform and the targeted service.

<table>
<thead>
<tr>
<th>Network flows (From -&gt; To)</th>
<th>Tenable’s usage (optional)</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable for AD SaaS</td>
<td>Email notifications</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td>platform -&gt; Support services</td>
<td>Syslog notifications</td>
<td>Syslog</td>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Tenable REST API</td>
<td>TLS /HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td></td>
<td>Identity provider</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>LDAP server</td>
<td>TCP/443</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>Identity provider</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636</td>
</tr>
</tbody>
</table>

### 4. Prerequisites

#### 4.1. Minimal configuration

The Tenable.AD_Cloud_technical_prerequisites_TLS_vX.X document describes the sizing requirements to run the solution. We do not support running Tenable.AD on a configuration smaller than these prerequisites.

<table>
<thead>
<tr>
<th>Tenable Security Probe - Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active AD users</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>1 – 25,000</td>
</tr>
<tr>
<td>25,001 – 50,000</td>
</tr>
<tr>
<td>50,001 – 75,000</td>
</tr>
<tr>
<td>75,001 – 100,000</td>
</tr>
<tr>
<td>100,001 – 150,000</td>
</tr>
<tr>
<td>150,001 – 300,000</td>
</tr>
<tr>
<td>300,001 – 500,000+</td>
</tr>
</tbody>
</table>

#### 4.2. Additional support information

- Tenable.AD works with Windows Server 2016 with the latest available update.
- Tenable.AD installer requires Local Administrator rights on Windows Server 2016. If the account used for the installation is not the built-in one, make sure that this account can run programs without restrictions.
- Tenable.AD services require Local Administrator rights to run local services on the machine.
● Tenable.AD requires a dedicated data partition. You must not run Tenable.AD on the OS partition to prevent system freeze if the partition is full.

● Tenable.AD must be considered as a black-box: Each machine must be dedicated to the product and not shared for another purpose.

● Tenable.AD can create any folder starting with the ‘Alsid’ or ‘Tenable’ prefix on the data partition. Therefore, do not create folders starting with ‘Alsid’ nor ‘Tenable’ on the data partition.

4.3. Installation programs

Tenable.AD installation program is available on the Tenable release portal (https://www.tenable.com/downloads/).

To configure the TLS installation, we provide another file that contains all the required certificates:

● certs.zip

This package contains the files required to perform installation/uninstallation/update and to reconfigure the solution with different IP addresses (if needed).

⚠️ We highly recommend rebooting all machines before starting a new installation.

Deployment on Windows Server (Full-Desktop Experience)

You must place the installation program in a valid location on each server to set up.

In the following example, on the Directory Listener TLS machine, we put it on the Desktop:

<table>
<thead>
<tr>
<th>Binaries location</th>
<th>Binaries content</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Users\Administrator\Desktop\</td>
<td>Desktop:</td>
</tr>
</tbody>
</table>

● You can activate extended debug logging with the following command (replace the first path with your installation program location, and the second with your log file path):

```
"C:\Users\Administrator\Desktop\Tenable.ad_3.X.X.exe" AI_DEBUGLOG=1 /L*V "E:\example.log"
```

Deployment on Windows Server Core

The installation is fully automated. To perform the installation:

● Run the following command (replace the path by your installer file location):

```
C:\Users\Administrator\Desktop\Tenable.ad_3.X.X.exe
```
II. **UPDATE PROCEDURE**

1. **Backup your system**

   **Warning:** Tenable strongly advises you to **make a backup of your databases and/or make a snapshot of your environment** prior to the update procedure.

2. **Update Directory Listener**

   During this step, the process will update the following applications:
   - Tenable component
     - Ceti

   **Expert Mode:** this configuration (TLS mode) requires checking the “Expert mode” box on the first installer window to display the additional feature.

   The update mechanism is fully automated.

   To perform the update, execute “Tenable.ad_v3.X.X.exe” with full Local Administrator privileges.
   1. Select “Expert mode” and click on the “Next” button.

   ![Welcome dialog box on Directory Listener](image)

   2. In the next dialog box, features and location are automatically preselected based on the previous installation. As previously mentioned, you can only select the DirectoryListener feature. Click on the “Next” button.
3. The installation program automatically fills in RabbitMQ’s IP address based on the previous version. You can check if this is consistent, then click on the “Next” button and update Tenable.AD.

4. At the end of the installation, **WAIT** until the server asks for a reboot. **Do NOT reboot it now!** Leave it like this for the moment and go to the next page.

2. **Start Directory Listeners services**

   Databases and SEN must be running before starting DL services. Wait for the signal from the Tenable DevOps team to reboot the machine and turn on the Ceti service.
III. **ACTIVE DIRECTORY CONFIGURATION**

1. General considerations

Tenable.AD is designed to be a non-intrusive solution able to monitor a directory infrastructure without requiring the deployment of agents, and as little as possible configuration change in the customer’s environment.

Tenable uses a regular user account with no administrative right to connect to standard APIs for its security monitoring feature (also named Indicator-of-Exposure), which by nature prevents any side effects for the monitored infrastructure. This feature leverages the Active Directory replication mechanisms to retrieve the relevant information which incurs limited bandwidth costs only between each domain’s PDC and Tenable DirectoryListener, but no additional cost within the infrastructure.

To efficiently **detect security incidents through its Indicator-of-Attack feature**, Tenable additionally leverages the ETW information (often used by Windows event logs) and the replication mechanisms available on each Domain Controller. To collect this set of information, a dedicated Group Policy object must be deployed using a dedicated deployment tool available in the Tenable console. This GPO activates, on all domain controllers, a WMI filter which will be written to the SYSVOL to profit from the AD replication engine and the Tenable’s ability to listen to SYSVOL events. Files written by the WMI filter are removed (using another WMI filter) as they are written using a rolling mechanism to avoid filling the SYSVOL.

To initiate security monitoring, Tenable.AD needs to contact standard directory APIs specified by Microsoft and documented in the MS-DRSR open specifications¹.

2. Access to specific Active Directory objects or containers

Tenable’s platform achieves its security monitoring without the need of administrative privileges. Despite its many advantages (operation safety, limited attack surface, etc.), this approach relies on the ability of the user account that the platform uses to read all the Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.). This section only applies for the platform benefiting from the Indicator-of-Exposure module.

By default, most of the objects natively benefit from a default read access for the group Domain Users used by Tenable’s service account. However, some containers need to be manually configured to allow read access to Tenable’s user account:

<table>
<thead>
<tr>
<th>Active Directory objects or containers requiring manual read access setup</th>
<th>Location of the container</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=Deleted Objects, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>Container hosting deleted objects</td>
<td></td>
</tr>
<tr>
<td>CN=Password Settings Container,CN=System, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>[Optional] Container hosting Password Strategy Objects</td>
<td></td>
</tr>
</tbody>
</table>

For each of the above containers, Tenable must grant access to the service account used by the platform via the following command line:

```
Command line

dsacls "<__CONTAINER__>" /takeownership

dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
```

In the previous table:

- `<__CONTAINER__>` refers to the container that requires access.
- `<__SERVICE_ACCOUNT__>` refers to the service account that the Tenable platform uses.

You must run this command on every domain monitored by Tenable’s platform.

3. Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack

This section only applies for the platform benefiting from the Indicator-of-Attack module and must be applied after each platform upgrade.

Tenable’s platform provides real-time security incident detection by correlating ETW information (generated by each domain controller) with LDAP and SYSVOL events. This section focuses on how to configure the monitored Domain Controllers to retrieve the required ETW information and to forward them to the Tenable.AD platform.

This section only applies for the platform benefiting from the Indicator-of-Attack module (IOA). It will first discuss:

- Tenable’s deployment script, a PowerShell script used to deploy Windows-component requirements on the Domain Controllers.
- How to install Microsoft Sysmon, a Windows system tool needed by some of the Tenable’s IOA to get relevant system data.
- How to uninstall or update Tenable’s deployment script.
- Potential issues with the audit policy.
3.1. Tenable’s deployment script

To retrieve the required ETW information within Tenable’s platform, we designed a unique system based on an agentless solution. This solution extracts ETW insertion strings\(^2\) data and forwards them, using a simple PowerShell script, to SYSVOL files. This approach only necessitates a one-time initialization step to:

- Set up the PowerShell script to execute.
- Configure the necessary audit policies.

This initialization step is performed on each domain controller using a Tenable deployment script downloadable in Tenable.AD, in System > Configuration > Indicator of Attack. This page lists the commands to execute (one for each domain registered in Tenable.AD). To activate the monitoring process, the Tenable deployment script will create a GPO that embeds an immediate task to configure the PowerShell ETW script, which runs on each DC to extract ETW information. This immediate task also installs a WMI filter to restart the PowerShell script at boot.

---

**We do not support manually deploying a GPO from one domain to another. Please use a Tenable deployment script for each domain you want to monitor.**

---

You launch the Tenable deployment script from a machine that is a member of the domain to monitor (some customers run the script directly from one of the Domain Controllers, which we also support), using an account with enough administrative privileges to create a GPO and to link it to the organizational unit hosting the Domain Controllers of the domain to monitor.

This machine must also have various PowerShell modules installed and available: ActiveDirectory and GroupPolicy. Note that the ActiveDirectory PowerShell module must also be available on each DC of the domain.

When installing the GPO, the deployment script checks for the replication status (a GPO cannot be installed while the DC is replicating). Therefore, the RSAT-DFS-Mgmt-Con feature is also necessary on the machine that runs this script.

Configuration adaptations

For each targeted domain, executing this Tenable deployment script applies configuration changes, listed below. You can modify some parameters (e.g. the GPO name) using command-line arguments passed when executing the script.

Use the following PowerShell command to have the complete list of available arguments and examples:

```
Command line
```

---

\(^2\) ETW insertion strings are the same information used by Windows to build its Event Logs
Synthesis of the technical changes made by Tenable’s deployment script

The following table describes the major configuration changes applied to the Domain Controllers to monitor. Created by the Tenable deployment script, the GPO applies these changes transparently.

<table>
<thead>
<tr>
<th>Configuration changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Add a GPO, named “Tenable.AD” by default, linked to the Domain Controllers OU by default. This GPO contains an immediate task configuring the PowerShell script running on each DC and installing a WMI filter that will start the PowerShell ETW script at boot, and the Advanced logging policy (see below).</td>
</tr>
<tr>
<td>• Activate the Microsoft Advanced logging policy, by modifying a registry key3 (using the GPO).</td>
</tr>
<tr>
<td>• Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable’s IOAs.</td>
</tr>
<tr>
<td>• Install a WMI event consumer that will execute a VBS script (using the ActiveScriptEventConsumer class). This VBS script is run at boot and looks for a running PowerShell ETW script, which it will run if not found.</td>
</tr>
</tbody>
</table>

The new event log policy is dynamically generated within the Tenable deployment script and activated by the GPO. You must apply this mandatory policy to have the ETW engine generate the Insertion Strings that Tenable requires. This policy does not disable any existing logging policy, but enriches them if necessary. If it detects a conflict, the Tenable deployment script stops with a message stating that the audit policy policy_name is needed, but the current AD configuration prevents its configuration.

More technical information describing step-by-step changes operated by Tenable deployment script is available in Tenable’s online documentation, reachable at https://docs.tenable.com/Tenablead.htm.

Limitation and potential impacts

Despite being the less intrusive way to capture Domain Controllers’ ETW information, some limitations and limited impact could exist in Tenable’s approach. Review these drawbacks before starting the deployment of the Indicator-of-Attack module.

Tenable’s incident detection module is based on the ETW data, thus bound by their limitations as defined by Microsoft4.

The installed GPO needs to be replicated over the entire domain, and the GPO refresh interval must finish for the install process to complete. During the replication period, false positives and false negatives can happen even though Tenable minimizes this effect by not starting the checks in the IOA engine immediately.

Tenable is using the SYSVOL file share to retrieve ETW information coming from the Domain Controllers. As the SYSVOL replicates to every Domain Controller of the domain, a significant increase in replication activity will appear during a high peak of AD activity.

Replicating files between the Domain Controllers and Tenable’s platform also consumes some network bandwidth. These impacts are mitigated by the automatic removal of the files that Tenable collects and the limited size of these files (500 MB maximum by default; see the MaxBufferSizeBytes script variable for the exact default value).

---

3 Specifically, the registry key is MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy, Set to 1
4 Microsoft documentation: https://docs.microsoft.com/en-us/windows/win32/etw/about-event-tracing#missing-events
3.2. Microsoft Sysmon

The additional Microsoft Sysmon service is required to activate a subset of Tenable’s Indicators-of-Attack. Supported by Microsoft, this software registers a new Windows Service to provide more security-oriented information in the ETW infrastructure.

The list of Indicators-of-Attack requiring Microsoft Sysmon to operate are listed in the following table. If the IOA is not mentioned, it will work even if Microsoft Sysmon has not been deployed.

<table>
<thead>
<tr>
<th>Indicators-of-Attack requiring Microsoft Sysmon</th>
<th>Name of the indicator</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Credential Dumping: LSASS Memory</td>
<td>Detecting Process Injection</td>
<td></td>
</tr>
</tbody>
</table>

Tenable understands that installing an additional Windows Service can affect the performance of the Domain Controllers hosting the AD infrastructure. Therefore, Tenable chooses not to automatically deploy Microsoft Sysmon. You must install it manually or use a dedicated GPO.

Manual deployment of Microsoft Sysmon on the domain controllers (optional)

![Warning]

**Sysmon deployment and management is at the customer's discretion. In particular, incompatibilities need to be tested before a full-blown deployment.**

1. Once downloaded from the Sysinternal website, run the following command to install Microsoft Sysmon on the current machine:

   **Command line**
   
   ```
   .\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
   ```

   **Note:** The configuration file is available in the annexes of this document or on Tenable's documentation portal where the file is entirely commented.

2. This Sysmon installation is not sufficient by itself. Add a registry key to indicate to the WMI filters that Sysmon is installing:

   **Command line**
   
   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
   ```

   **Note:** In case Sysmon does affect the performance of the AD infrastructure, run the following command to uninstall Sysmon from the current machine:

   **Command line**
   
   ```
   ```

---

6 Sysinternal website: [https://docs.microsoft.com/en-us/sysinternals/](https://docs.microsoft.com/en-us/sysinternals/)
7 Tenable documentation portal: [https://docs.tenable.com/Tenablead.htm](https://docs.tenable.com/Tenablead.htm)
3.3. Problem with Advanced Audit Policy Configuration GPO precedence

The GPO created by Tenable.AD to enable required events logging is linked to the Domain Controllers OU and Enforced mode is enabled.

This gives it a very high priority, but an Enforced GPO configured at a higher level (e.g. Domain or Site) takes precedence over it. If this higher priority GPO defines the Advanced Audit Policy Configuration settings that conflict with Tenable’s needs, it will win and Tenable.AD will miss required events for attack detection.

Advanced Audit Policy Configuration settings defined by GPOs are merged by Windows, so different GPOs can define different settings. However, at each setting level, only the value defined by the GPO with the higher precedence is used. For example, Tenable.AD needs the "Success and Failure" value for the "Audit Credential Validation" setting. However, if a GPO with more precedence only defines "Success" for "Audit Credential Validation", then Windows will only collect "Success" events and Tenable.AD will miss the required "Failure" too.

How to check?

1. Run the following command on a Domain Controller. It will output the effective Advanced Audit Policy Configuration after considering all GPOs and precedence.

```
	.
Sysmon64.exe -u
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
```

```
Command line

auditpol.exe /get /category:*
```

2. Compare the output with the Tenable.AD advanced audit policy requirements:
   - For each setting required by Tenable.AD, ensure that the effective policy covers it, at least.
This is also fine if the effective policy is more exhaustive, for example when Tenable.AD needs "Success" or "Failure" and the setting is "Success and Failure".

**How to fix it?**

If the effective policy is insufficient, it means that a GPO with a higher precedence defines conflicting settings. Look for GPOs linked to higher levels (Domain or Site) in Enforced mode that define Advanced Audit Policy Configuration.

1. Run the following command on a Domain Controller to pinpoint the Winning GPO:

   **Command line**
   ```
gpresult /scope:computer /h gpo.html
   ```

2. Once you identify it, you must modify the corresponding Advanced Audit Policy Configuration setting in the GPO to cover at least what Tenable.AD requires.
   - For example, if Tenable.AD requires "Success" and the higher priority GPO defines "Failure", then modify it to "Success and Failure".
   - If Tenable.AD requires "Success and Failure" and the higher priority GPO defines "Success", then modify it to "Success and Failure".

3. After modification, wait until the updated GPO applies, or force it with the "gpupdate" command.

4. Check the new effective policy as instructed above.

**3.4. Update the Tenable module on the Domain Controllers**

To update the Tenable’s IoA module, you must:

1. Uninstall the script currently in use by running it with the "-Uninstall" parameter.
2. Wait a few hours so the cleaning GPO is properly replicated and applied by all domain controllers (at the time of writing, the script will enforce a 4-hour delay).
3. Delete manually the cleaning GPO.
4. Download the new script version.
5. Install it as explained above.
IV. **ANNEXES**

1. **Optional Sysmon configuration file**

```xml
<Sysmon schemaversion="4.40">
  <EventFiltering>
    <!-- SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate] -->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged -->
      </ProcessCreate>
    </RuleGroup>
    <!-- SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime] -->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </FileCreateTime>
    </RuleGroup>
    <!-- SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect] -->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </NetworkConnect>
    </RuleGroup>
    <!-- SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES -->
    <!-- Cannot be filtered. -->
    <!-- SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate] -->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged -->
      </ProcessTerminate>
    </RuleGroup>
    <!-- SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad] -->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </DriverLoad>
    </RuleGroup>
    <!-- SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad] -->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </ImageLoad>
    </RuleGroup>
    <!-- SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread] -->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <!-- TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe"/>
      </CreateRemoteThread>
    </RuleGroup>
    <!-- SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead] -->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </RawAccessRead>
    </RuleGroup>
    <!-- SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess] -->
    <RuleGroup name="" groupRelation="or">
      <ProcessAccess onmatch="include">
        <!-- Detect Access to LSASS -->
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1FFFFF</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1F1FFF</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1010</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x143A</GrantedAccess>
        </Rule>
        <!-- Detect process hollowing to LSASS -->
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x0800</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1810</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <!-- Detect process hollowing to LSASS -->
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1800</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1083,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe"/>
          <GrantedAccess>0x1438</GrantedAccess>
        </Rule>
      </ProcessAccess>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```
<GrantedAccess>0x800</GrantedAccess>
</Rule>

<!-- Detect process process injection to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x0820</GrantedAccess>
</Rule>

<!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
<RuleGroup name="" groupRelation="or">
  <FileCreate onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreate>
</RuleGroup>

<!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
<RuleGroup name="" groupRelation="or">
  <RegistryEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RegistryEvent>
</RuleGroup>

<!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
<RuleGroup name="" groupRelation="or">
  <FileCreateStreamHash onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreateStreamHash>
</RuleGroup>

<!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
<RuleGroup name="" groupRelation="or">
  <FileCreate onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreate>
</RuleGroup>

<!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
<RuleGroup name="" groupRelation="or">
  <WmiEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </WmiEvent>
</RuleGroup>

<!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
<RuleGroup name="" groupRelation="or">
  <DnsQuery onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </DnsQuery>
</RuleGroup>

<!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
<RuleGroup name="" groupRelation="or">
  <FileDelete onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileDelete>
</RuleGroup>

</EventFiltering>
</Sysmon>